



MD MVA eFR-19 Remote Access Request Form

REQUESTER INSTRUCTIONS:

DATE of REQUEST :

Complete top section of form, listing each "Insurer" company you are authorized to issue Maryland Insurance Certifications (Form FR-19), "SignDate" sign, and date. This request may require approval from your Insurance Company or Agency Officer. Mail to ICD Business Administrator at MVA Room 140, 6601 Ritchie Hwy, Glen Burnie, MD 21062, for authorization signature. ICD Business Administrator will submit signed form to MVA Security Officer for verification of access type(s).

ACTION: ☐ New Request ☐ Account Change ☐ Account Deletion ☐ Add Insurer Association ☐ Remove Insurer Association

USERID: _____ (assigned by MVA) Producer License No issued by MD Ins Admin _____

MD Insurance Agent: _____ Phone: () _____
Last First MI Suffix

Ins Co / Agency Name: _____ Address: _____

Agency Phone Number: () _____ Agency Fax Number: () _____

E-Mail Address: _____

Insurer's Agent is Authorized to Issue Maryland Insurance Certifications (form FR-19) for: (use additional sheet if more than 6 insurers)

Insurer NAIC Code is the 5 Digit Number assigned by the National Association of Insurance Commissioners

Insurer NAIC	Insurer Name	Insurer NAIC	Insurer Name
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____

Purpose of Remote Access: To report Maryland Insurance Certifications Forms FR-19 electronically to Insurance Compliance Division.

ACKNOWLEDGMENT: Remote Access to the MDOT/MVA network is a privilege. I hereby acknowledge that remote access is authorized for my use only and that all passwords and user names are to be kept confidential at all times. By requesting a remote access account, I acknowledge that I will install or already have installed virus protection software on my remote (this includes business, home or laptop) system. In addition, I authorize MVA and/or their contractor to test the security of my connection to the MVA network by performing a coordinated vulnerability assessment when needed of my connection to the MVA network. Installation of the virus protection and applying virus signature updates is my responsibility. I understand that failure to do so may result in loss of remote access privileges. MVA employees are not responsible for any operating system, hardware or software application problems encountered by any MVA Remote Access User when using the designated applications to connect to the MVA network. I have signed the MDOT Security Advisory agreement and I am aware of terms and conditions of the agreement.

Requester Signature/Date: _____

=====

INSURANCE CO/AGENCY OFFICER: I authorize the requestor to be granted access to the MD ACIS eFR-19 Internet application.

ON BEHALF OF INSURANCE COMPANY AGENCY _____

INSURANCE CO/AGENCY OFFICER Name & Title (Please Print): _____

INSURANCE CO/AGENCY OFFICER Signature/Date: _____

=====

MD MVA ACIS BUSINESS ADMINISTRATOR: I authorize the requestor to be granted access to the ACIS eFR-19 internet application.

MVA ACIS Business Administrator Name (Please Print): _____

MVA ACIS Business Administrator Signature/Date: _____

IMPLEMENTATION DETAILS (TO BE COMPLETED BY MVA ONLY)

MVA Security Officer Signature/Date: _____

MARYLAND DEPARTMENT OF TRANSPORTATION
OTTS OFFICE OF DATA SECURITY
SECURITY ADVISORY

This ADVISORY is initiated for INFORMATIONAL purposes only. The following paragraphs shall in no way be construed as a waiver by an employee of the rights and protections provided to employees by the Merit System Law (Article 64A of the Annotated Code of Maryland).

The Office of Information Resources and its Client/Agencies adhere to the State Policy: Data Processing Resources Security, as authorized by the Governor's Executive Order 01.01.1983.18; the State Data Security Committee, State Agency Data System Security Practices; Article 27, Section 45A and 146 of the Annotated Code of Maryland. In addition, other Federal and State Laws and Regulations affect the access to and use of computer information such as the U. S. Computer Crime Statute (1984), Computer Security Act of 1987, National Driver Register Act of 1982 (Public Law 97-364), Privacy Act of 1974, Freedom of Information Act, Computer Software Rental Amendments Act (1990), Fair Credit Reporting Act, Computer Fraud and Abuse Act (1986), Federal Driver Privacy Act 1994; 18 U.S.C. '2720 et seq. and, with "10-611, 10-616, 10-626 of the State Government Article; '12-111 through 12-113 of the Transportation Article, Annotated Code of Maryland, which limit access to personal information from public records in Maryland and Federal Copyright Law.

Specifically **PROHIBITED ACTS** include, but are not limited to:

1. Unauthorized access to or use of a computer, data or software.
2. Unauthorized copying or disclosure of data or software.
3. Obtaining unauthorized confidential information.
4. Unauthorized modification or altering of data or software.
5. Introduction of false information (public records).
6. Disruption or interruption of the operation of a computer.
7. Disruption of government operations or public services.
8. Denying services to authorized users.
9. Taking or destroying data or software.
10. Creating/altering a financial instrument or fund transfer.
11. Misusing or disclosing passwords.
12. Breaching a computer security system.
13. Damaging, altering, taking or destroying computer equipment or supplies.
14. Devising or executing a scheme to defraud.
15. Obtaining or controlling money, property, or services by false pretenses.

Authorized access to, including **INTERNET** and **INTRANET**, and use of information and computer resources is limited to the **PURPOSE** for which these privileges are granted. All authorized users during the term of their access and thereafter, shall hold in strictest confidence and not willfully disclose to any person, firm or corporation without the express authorization of the Director, OIR, any information related to security, operations, techniques, procedures or any other security matters. Any breach of security will be promptly reported to the Director, Office of Information Resources, designee or security officer.

I acknowledge that I have read and understand the foregoing security advisory.

Date: _____

Name: _____

(Please print or type)

SSN: _____

(Signature)